AU/ACSC/0603/97-03

INFORMATION WARFARE:

COMBATING THE THREAT IN THE 21ST CENTURY

A Research Paper

Presented To

The Research Department

Air Command and Staff College

In Partial Fulfillment of the Graduation Requirements of ACSC

by

Major Mary M. Gillam

March 1997

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense.

Contents

Illustrations

Page

Preface

Military history is replete with examples of how critical information about one's adversary has played an important role in combat. For example, military strategists such as Sun Tzu and Hannibal used spies to obtain key information about their enemies. However, the coalition victory in Operation DESERT STORM would take information superiority to a higher level rivaling anything in history. This new form of warfare classified as "Information Warfare" (IW) proved to be a force multiplier in helping the allies defeat the world's fourth largest military force.

Why should we be concerned about IW? Our nation's growing dependency on information and information-based technologies creates tremendous vulnerabilities in our national security infrastructure. A hostile adversary can wage IW attacks anonymously from the global sphere. These attacks can quickly paralyze a nation that is severely dependent on information and information systems.

Our nation's commitment to combating this new form of warfare is paramount, thus making IW a critical area of study. I have only touched the surface, and I hope future Air Command and Staff College students will continue the quest.

I would like to thank Lt Col Jim Near and Lt Col Tim Ryan for their guidance and wisdom. Their ability to help me focus my research enabled me to create a product of importance to Air Command and Staff College and the nation.

Abstract

As we approach the dawn of the 21st century, success of our national security strategy will depend greatly on our ability to combat the Information Warfare (IW) threat. Old paradigms regarding conventional warfare must change to incorporate this new form of warfare. Our nation's growing dependency on information and information-based technologies has made IW a legitimate weapon for potential adversaries. The "information" and its support infrastructures are becoming extremely vulnerable to hostile attacks. Adversarial forces can now wage information-based warfare from anywhere in the world, and literally remain anonymous. Thus, our ability to recognize and defend against this new form of warfare is paramount to the survival of our national security infrastructure.

Thesis Statement

The thesis of this research project is predicated upon the following premises: First, the exploitation of "information" as a weapon is changing the nature of warfare. Second, although there is much debate about the reality of the IW threat, this paper postulates that adversarial IW tactics pose a legitimate threat to our national security infrastructure. Finally, the Department of Defense (DOD), the Joint Staff, and the Services must remain actively committed to combating the IW threat in the 21st century.

Research Methodology

The roadmap for this research project is as follows: Chapter 1 limits the scope of the IW study and provides a common frame of reference upon which to build the remainder of the paper (i.e. definitions, concepts). Chapter 2 discusses the changing nature of warfare. Chapter 3 analyzes the IW threat. Chapter 4 examines the DOD, the Joint Staff and the Services' IW activities. Chapter 5 provides recommendations for improving our ability to combat the IW threat in the 21st century (i.e. education, training). Chapter 6 concludes with a summary of my research findings.

Research for this project was conducted in several ways. Several primary and secondary sources were used to complete the project. The Information Warfare elective taught by Lt Col Near and Lt Col Ryan was a tremendous source of key information. The most noteworthy primary source was *Information Warfare: Legal, Regulatory, Policy and Organization Considerations for Assurance* developed by the Science Applications International Corporation (SAIC) for the Joint Staff. Publications by IW enthusiasts Martin C. Libicki and Winn Schwartau were also used. *The First Information War* by Alan D. Campen provided great insight on Operation DESERT STORM. Several joint publications, professional magazines (i.e. SIGNAL) and the Internet were particularly useful for understanding how DOD, the Joint Staff, and the Services are working to combat the IW threat.

Chapter 1

Introduction

> *Information Warfare has emerged as a key joint warfighting mission area. The explosive proliferation of information-based technology significantly impacts warfighting across all phases, the range of military operations, and all levels of war.*
>
> — Gen John M. Shalikashvili
> Chairman, Joint Chiefs of Staff

The end of the Cold War was a historical triumph for the North Atlantic Treaty Alliance. The threat of a nuclear holocaust had declined. Member nations were now free to focus their political and military might on internal problems within their own nation's boundaries.

Unfortunately, Operation DESERT STORM would reveal the existence of a new kind of threat and a new type of warfare which we have come to know as "Information Warfare" (IW). Many military scholars have identified Operation DESERT STORM as the first information war.[1] Consequently, this identification has led military strategists to an intense study of this new form of warfare. Paul Nitze, one of the architects of the Cold War strategy stated:

> The Gulf War offered a spectacular demonstration of the potential effectiveness of smart weapons used in a strategic role. Against Iraq, such weapons rapidly rendered useless the military forces of a powerful dictator, in particular by neutralizing his command, control and communications facilities.[2]

The purpose of this research project is to examine the IW threat and its impact on the Department of Defense (DOD), the Joint Staff and the Services. The paper will address this issue by answering several questions: First, how has IW changed the nature of warfare? Second, is the threat perceived by IW real or imagined? Finally, what has DOD, the Joint Staff, and the Services done to combat this new wave of warfare? After answering these questions, the paper will make recommendations about how these organizations can improve their ability to combat the IW threat and present a few concluding comments.

Chapter 1 will establish a foundation upon which to build the remainder of the paper. For example, critical terms and concepts will be explained before proceeding on into the paper. Chapter 2 will discuss the history of war and its changing nature. Chapter 3 will address the IW threat facing our Armed Forces. Chapter 4 will review the IW activities occurring within the DOD, the Joint Staff and the Services. Chapter 5 will present recommendations that will enable DOD, the Joint Staff and the Services to better prepare to combat the IW threat. Finally, chapter 6 concludes with a summary of the findings.

Definitions

To establish the proper framework from which to examine Information Warfare, it is imperative that certain terms (i.e. information, information system, information warfare) be explained. In addition, a basic understanding of how information is transmitted is also provided for clarification.

Joint Pub, 6-0, defines information as "data collected from the environment and processed into a useable form."[3] The information is the critical output of the information

system. In his book, *Joint Training for Information Managers*, Col Arthur G. Maxwell, Jr., a career Army signal officer, quoted General Colin Powell on the importance of information. General Powell said "information is the life blood of an organization and effective communications can support the war fighter as a combat multiplier."[4] Warfighters depend on information for planning operations, executing missions, and deploying forces. This information is crucial for commanders in developing their commander's intent during campaign planning. Since a commander's intent is transmitted two echelons above and below him, it is imperative that the information is accurate. Thus, information can become a valuable target for an adversary to exploit.

Now that we have defined information, let's now take a look at a information system? According to DOD Directive 3600.1 a information system is defined below:

> The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infrastructure, organizations, and components that collect, process, store, transmit, display, and disseminate information.[5]

The US Armed Forces have become increasingly dependent on information systems. Much of this technology is commercial-off-the-shelf (COTS) products which were designed primarily for the commercial user. Thus, the level of security required for certain military applications is not resident in many of the COTS products.

The most important term that we need to define is IW. What is it? Is it the new "buzz word" for the 21st century or is it a legitimate type of warfare? The market is flooded with books on the subject and thus definitions are multifarious. Winn Schwartau, author of *Information Warfare: Chaos on the Electronic Superhighway* defined IW as "an electronic conflict in which information is a strategic asset worthy of conquest or

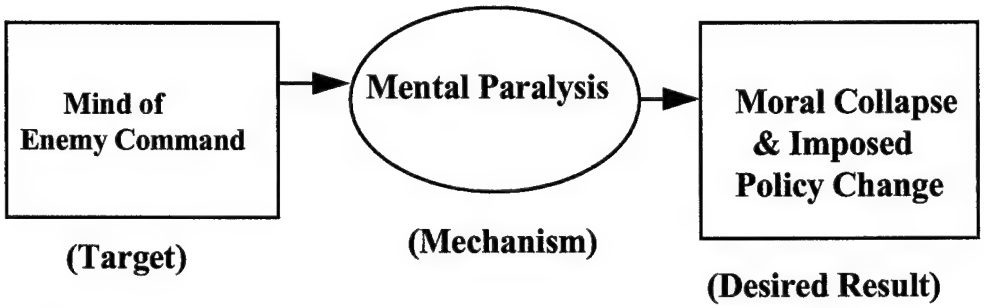
destruction."[6] In September 1995, the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I), Lieutenant General (ret) Emmett Paige, Jr., published the following unclassified definition of Information Warfare:

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks.[7]

The above definition suggests that IW involves both offensive and defensive measures. Offensive measures are those taken to affect an adversary's information and information systems, while defensive measures are those actions taken to protect our own information and information systems.[8] A successful IW strategy must incorporate both measures. They must work coherently to produce a synergistic effect that will erode a potential hostile commander's decision-making cycle.

Colonel (ret) John Boyd is well-known for his theory regarding this decision-making cycle. He postulates "that all rational human behavior, individual or organizational, can be depicted as a continual cycling through four distinct tasks: observation, orientation, decision, and action (OODA)."[9] This continuing cycle forms what he calls a OODA loop. The winner in this interchange is he who can infiltrate his opponent's OODA loop more quickly and more accurately.

Political scientist Robert Pape developed an analytical model to graphically depict and simplify Col Boyd's theory. His model is shown in figure 1.



Source: Major David S. Fadok, *John Boyd and John Warden, Air Power's Quest for Strategic Paralysis* (Air University Press, MAFB, AL. 1995, 17.

Figure 1. John Boyd's Theory of Conflict

As the model indicates, the mind of the enemy leadership becomes a potential target. Mental paralysis is the mechanism used to accomplish the desired result. From the model, it is easy to see how IW tactics directed at the appropriate target can affect the commander's decision-making capability.

Additionally, IW tactics can also target the communications system used to transmit the information to the commander. Thus, a basic knowledge of a communications system will aid in understanding the vulnerabilities in this system.

Basic Communications System

The basic communications system contains four major components: "terminal devices, transmission media, switches, and control and management."[10] Figure 2 contains a graphic depiction of this system. A computer represents a terminal device. Information exchanged between terminal devices travel over various types of transmission media (i.e. radio, metallic wire, fiber-optic cable). Switches are used to route the information over the network from one place to another. The final component, control and management is crucial for network and nodal control. "Network control provides management of area,

regional, theater, or global networks, while nodal control provides management of local command, control, communications, and computer systems."[11]

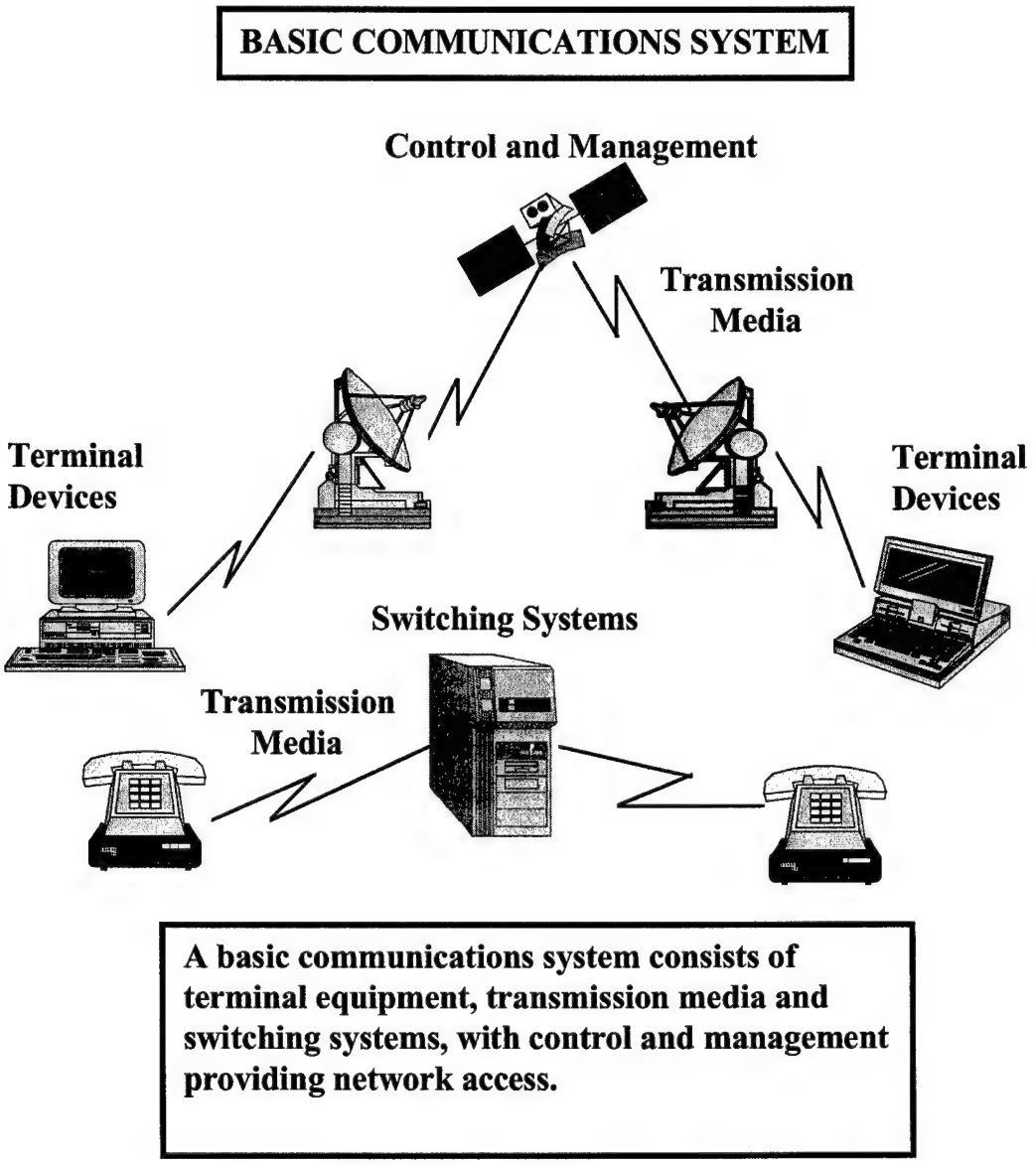


Figure 2. Basic Communications System

Summary

Operation Desert Storm ushered in a new form of warfare: Information Warfare. Military theorists worldwide contribute the coalition victory in the Gulf to a successful

information superiority campaign. However, future wars may involve rogue nations or terrorist organizations capable of orchestrating IW attacks against our information, air traffic control, or economic infrastructures. The DOD, the Joint Staff, and the Services will have to combat this new threat in the 21st century.

The purpose of this chapter was to lay a basic terminology foundation upon which to build the remainder of the paper. Several definitions (i.e. information, information system, information warfare) were presented for clarification. Col (ret) John Boyd's strategic paralysis theory was discussed in relations to its impact on the commander's decision-making process. Finally, a basic understanding of a communications system was presented to show how attacking any of these components can render information unreliable. The next chapter will now discuss how conventional warfare has changed to reflect the IW character of war.

Notes

[1]Alan D. Campen, *The First Information War* (Fairfax VA: AFCEA International Press, October 1992) ix.

[2]Quoted in Command, Control, and the Common Defense, revised edition by Kenneth Allard, *Desert Storm and Information Age Warfare*, 273.

[3]Joint Pub 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, 30 May 95, I-3.

[4]Arthur G. Maxwell, Jr., *Joint Training for Information Managers, National Defense University*, May 1996, xiii.

[5]*Information Warfare: Legal Regulatory, Policy and Organization Considerations for Assurance*; research report by SAIC for J6K, 4 July 1996, B-73.

[6]Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994) 13.

[7]Col Brian Fredericks, *Information Warfare: The Organizational Dimension* (U.S. Army War College, Carlisle Barracks, Pennsylvania, 7 Feb 96) 2.

[8]JCS Publication, *Information Warfare: A Strategy for Peace...The Decisive Edge in War*, 1997, 6.

[9]Major David S. Fadok, *John Boyd and John Warden, Air Power's Quest for Strategic Paralysis* (Air University Press, MAFB, AL. 1995, 16.

Notes

[10]Joint Pub 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations,* 30 May 1995, II-2.

[11]Ibid., II-3.

Chapter 2

Changing Nature of Warfare

Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adopt themselves after a change occurs.

—Guilo Douhet

Will conventional warfare remain the norm for the 21st century or will a new wave of warfare emerge? This chapter begins by discussing the history of warfare through the eyes of two popular futurists, Alvin and Heidi Toffler. It later addresses how warfare has changed thus causing DOD, the Joint Staff, and the Services to evolve to meet this new form of warfare.

History of Warfare

Down through the corridors of time, wars have been fought for various reasons. Conflict arose from regional instabilities, economic and social perils, and religious animosities. In their book, *War and Anti-War: Survival At The Dawn of The 21st Century*, Alvin and Heidi Toffler categorize the evolution of warfare into three stages or waves: agrarian, industrial, and informational.[1] Colonel Owen E. Jensen summarized the description of these stages of warfare in his work, *Information Warfare: Principles of Third Wave War.*

> In the history of man, three basic types of warfare have evolved: agrarian, industrial, and informational. First came the agrarian warfare. When man learned to grow food, he no longer had to wander and hunt. Populated towns developed, and the practice of hoarding a surplus of food became possible. It was then that true warfare, [a bloody clash between organized states] began. Weapons, hand held and hand-crafted, were agrarian. The agrarian goals of capturing surplus wealth and land justified and motivated wars. Wars followed agrarian patterns, being fought only during intervals between reaping and sowing. And technology changed, but slowly overtime. Agrarian warfare principles were espoused by a well-known guru, Sun Tzu. Much of what he wrote was timeless, and much pertained only to agrarian warfare.
>
> The agrarian economic and military climate began to change in the seventeenth century with the introduction of steam power. This change accelerated with the growing manufacture of interchangeable, machined parts. It flowered with urban development, the French Revolution, the levee en masse, and the concept of a "nation in arms." We call this era the industrial age, and with it came industrial warfare. Here we find standardized weaponry, professional full-time soldiers, mass production, mass destruction, and goals echoing the Darwinian industrial economic struggle: annihilation, unconditional surrender, and subordination. Once again, we know the guru of this era, Carl von Clausewitz. Much of what he wrote is timeless, and much pertained only to industrial warfare.
>
> While some areas of the world remain in the agrarian realm and others have advanced only to the industrial state, a few have broken out into a completely new era—the **information age**.[2]

Information—The New Battlespace Weapon?

Many theorists believe we are in the midst of an information age. Although the weapons of warfare have changed, the ultimate objective remains the same: conquering one's adversary. The information age has created new targets of opportunity thus changing the way in which war in the 21st century will be fought.

For example, what happens when the new battlespace frontier becomes the mind of the individual commander and the information he uses to make critical decisions? George Gilder, author of *The Quantum Revolution in Economics and Technology*, said "the most

valuable capital is now the capital of human mind and spirit."[3] Dr George J. Stein, director of International Security Studies at Air War College, Maxwell Air Force Base, Alabama, said "The target of Information Warfare...is the human mind, especially those minds that make key decisions of war or peace."[4]

When we think of the mind, thoughts of Plato and Aristotle surface to the forefront. The mind and its mental processes have fascinated philosophers throughout the ages. Random House defines the mind as "the agency or part in a human or other conscious being that reasons, understands, wills, perceives..."[5] Man is distinguished from the rest of nature by his highly developed capacity for thought. His ability to rationalize and process information received are characteristics of a sound mind. The "information" becomes the centerpiece of this transaction. However, when the information becomes damaged, corrupted or unreliable, it threatens his ability to make sound and accurate decisions. IW, thus with its focus on destroying information becomes a legitimate and perhaps preferred tactic for use by potential adversaries.

British armor theorist, J.F.C. Fuller, author of the famous tank Plan 1919 recognized the benefits of attacking the brain within an organization. He believed that attacking the brains of an organization and severing it from the remainder of its organization would produce enough chaos to create what he called "strategic paralysis."[6] Although he referred to the brain as the headquarters' unit, it is easy to understand how disrupting the information flow can paralyze a warfighting force.

Although there is much evidence to suggest that the information age has changed warfare, in his book, *What is Information Warfare*, Martin Libicki describes the difficulty involved in determining the nature of IW.

> In the fall of 1994, I was privileged to observe an Information Warfare game sponsored by the Office of the Secretary of Defense. Red, a middle-income nation with a sophisticated electronics industry, had developed an elaborate five-year plan that culminated in an attack on a neighboring country. Blue, the United States, was the neighbor's ally and got wind of Red's plan. The two sides began an extended period of preparation during which each conducted peacetime information warfare and contemplated wartime information warfare. Players on each side retreated to game rooms to decide on moves.
>
> Upon returning from the game rooms, each side presented its strategy. Two troubling tendencies emerged: First, because of the difficulty each side had in determining how the other's information system was wired, for most of the operations proposed (for example) no one could prove which actions might or might not be successful, or even what "success" in this context meant. Second, conflict was the sound of two hands clapping, but not clapping on each other.
>
> Blue saw information warfare as legions of hackers searching out the vulnerabilities of Red's computer systems, which might be exploited by hordes of viruses, worms, logic bombs, or Trojan horses. Red saw information warfare as psychological manipulation through media. Such were the visions in place even before wartime variations on information warfare came into the discussion. Battle was never joined, even by accident. This game illustrated a fundamental difficulty in coming to terms with information warfare, deciding on its nature.[7]

Although the nature of IW may be in question, "History tells us that with each phase of new technology comes a new type of crime."[8] The advances made in technology over the past decade have enabled our military to literally revolutionize the battlefield. The Army's *Force XXI,* the Navy's *Forward...From the Sea,* and the Air Force's *Global Engagement: A Vision for the 21st Century Air Force* represents the Service's architectures for implementing this new technology. However, as these architectures are implemented over the next several years, our growing dependency on this technology will create open-doors for potential attacks by hostile adversaries.

Let's look at an example of a hypothetical IW situation. Suppose a terrorist organization wanted to influence the will of the American populace regarding a specific

situation. A possible course of action would be to infiltrate the computer systems of the Cable News Network (CNN), and begin sending something as simple as subliminal messages through the network. This scenario may appear improbable; however a few years ago, subliminal practices were carried out in the music industry. Several news broadcasts reported customers complaining of hidden messages being discovered in cassette recordings. For irrational actors such as terrorist organizations, nothing is beyond their scope of reason.

Summary

This chapter postulated that Information Warfare has changed the way in which wars will be fought in the future. Aside from targeting the commander's information and his information-based technologies, adversaries are also targeting the human mind to carry out their IW attacks. According to the Joint Staff, "Rapidly advancing information-based technologies and an increasingly competitive global environment have thrust information into center stage in society, government, and warfare in the 21st Century."[9] Lieutenant General Jay Garner, commander, Army Space and Strategic Defense Command said "One day, national leaders will fight out **virtual wars** before they decide to go to war at all."[10] The next chapter will examine the IW threat in more detail and its impact on the DOD, the Joint Staff and the Services.

Notes

[1]Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Little, Brown and Company, 1993) 23.

[2]Col Owen E. Jensen, *Information Warfare: Principles of Third Wave War* (Air Power Journal, 1994) 36.

Notes

[3]George Gilder, *Microcosm: The Quantum Revolution in Economics and Technology* (Simon and Schuster, New York 1989) 12.

[4]George J. Stein, quoted in *Airpower and Campaign Planning*, vol. 8, 215.

[5]Random House Dictionary (1980) 849.

[6]*Air Command and Staff College Seminar Book*, vol. 3, ver. 9, 10-77.

[7]Martin C. Libicki, *What is Information Warfare* (Washington, D.C.: National Defense University, 1996) 1-2.

[8]Garry S. Howard, *Introduction to Internet Security: From Basics to Beyond* (Prima Publishing, 1995) 102.

[9]JCS Publication, *Information Warfare: A Strategy for Peace...The Decisive Edge in War,* 1997, 1.

[10]Quoted in World Politics, Article by Douglas Waller *Onward Cyber Soldiers*, 96/97, 27.

Chapter 3

Global Threat

The threat to our military and commercial information systems poses a significant risk to national security and is being addressed.

—1996 National Security Strategy

The threats faced by our Armed Forces in the 21st Century will originate from many sources. Joint Vision 2010 states "The U.S. must prepare to face a wider range of threats, emerging unpredictably...and challenging us at varying levels of intensity."[1] According to Hans Binnendijk, director of the Institute for National Strategic Studies at the National Defense University and editor-in-chief of Joint Force Quarterly, "Terrorism will continue to threaten Americans especially members of the military."[2] This chapter will specifically address the IW threat (real or imagined) and its impact on DOD, the Joint Staff, and the Services.

How Real Is the IW Threat?

According to the US Security Policy Board, the following observation was made:

> The end of the Cold War has dramatically changed the threats that defined the security policies and procedures for protecting our government's information, facilities and people. While some threats have been reduced, others have remained relatively stable or have increased. Technologies, such as those used to create weapons of mass destruction are evolving and proliferating. With this greater diversity of threats, there is wide

> recognition that the security policies, practices, and procedures developed during the Cold War must be reexamined and changed."[3]

The exponential growth in information reliance and information-based technology has made Information Warfare (IW) a valid threat in the next century. For resource-limited adversaries, IW becomes a relatively cheap and practicable alternative to full-scale war. Since IW can be waged from anywhere in the global spectrum, it offers anonymity to potential adversaries. Our ability to prosecute these attackers is very limited due to regulatory and political dilemmas. Thus, IW becomes a legitimate war-making strategy capable of inflicting a vast array of damage upon its victims.

In a speech at the International Electronic Warfare (EW) Technical Symposium and Convention, the ASD/C3I, Lieutenant General (ret) Emmett Paige, Jr., stated the following:

> The availability and global proliferation of computer and telecommunications technology has put the tools of Information Warfare into the hands of any nation, organization or actor with hostile intentions.
>
> In addition to the traditional threat posed by historical adversaries and regional demagogues, we are seeing the potential rise of the "unstructured" threat—from the factional terrorist groups, to the economically-motivated electronic mercenary, down to the ego-driven hacker.
>
> The intelligence infrastructure is evolving into a form suited to analysis and characterization of the traditional threat. We are in the early stages of building an indications and warning system for IW analysis, coordination and damage assessment. However, the unstructured threat presents both a challenge and an opportunity for change.[4]

Recognition of the IW Threat

According to the Joint Staff, "To get to the essence of the IW threat requires an understanding of three elements: identities and intentions of possible attackers; possible

attack techniques and methods; and finally potential targets, extending from the strategic to the tactical levels."[5]

A potential adversary's identity is becoming extremely complex. Martin Van Creveld, author of *The Transformation of War* said, "In the future, war will not be waged by armies but by groups whom we call terrorists, guerrillas, bandits, and robbers."[6] It will take a concerted effort on the part of the intelligence community, law enforcement, and private enterprise to adequately identify the threat.

In *Information Warfare: A Strategy for Peace...The Decisive Edge in War*, the Joint Staff identified several potential IW targets as shown in figure 2. If military theorist Carl von Clausewitz were alive today, he probably would have classified these targets as critical centers of gravity. Successful IW attacks against these targets would undoubtedly devastate even the most powerful Armed Forces.

Leadership	Military Infrastructure	Civil Infrastructure	Weapons Systems
Key Personnel	Commanders	Communications (Links/Nodes)	Planes
ADP Support	C2 Communications Links	Industry	Ships
Strategic Communications	C2 Nodes	Financial	Artillery
Power Base	Intelligence Collectors	Populace	Air Defense

Source: JCS Publication, *Information Warfare: A Strategy for Peace...The Decisive Edge in War,* 1997 13.

Figure 3. Examples of IW Targets

How Vulnerable are We?

In an article in SIGNAL magazine entitled Defense Organization Safeguards War Fighters' Information Flow in October 1995, it was noted that the Defense Information

Systems Agency (DISA) Center for Information Systems Security (CISS) countermeasures department had launched 12,000 attacks against the Defense Department computer systems in 28 command vulnerability assessments. According to Michael Higgins, the CISS countermeasures department head, "more than 88 percent of those systems were successfully compromised. Only about 500 users detected the intrusions, and only two dozen users reported the intrusions."[7] The tools used to conduct the intrusions are readily available on the public market. Higgins also stated the following:

> The information security problem is worsening, as the number of computers in the US government continue to rise. The United States is the world's most interconnected country, and the operational reliance on computers also is increasing, along with the complexity of the computing environment. While active information security is being used, hackers who are motivated by money are turning professional.[8]

According to Clarence A. Robinson, Jr., editor-in-chief of SIGNAL magazine "computer crime is viewed as the fastest growing component of global organized crime. At least 122 nations have computer espionage programs, and the computer underground considers the Defense Department [easy pickings].[9]

Additionally, the Department of Defense is extremely dependent on the Internet which is described below:

> The Internet is a worldwide network of interconnected computer systems and sub-networks providing access on the largest scale. There are 90 domains globally, with more than 3.8 million hosts and an estimated 40 mission users. The Internet is growing at a rate of 168 percent per year worldwide, and at 183 percent a year in foreign nations.
>
> There are 56,000 networks in 86 countries connected to the Internet, and 154 countries have electronic mail links. In the United States alone, seven domains have 2.5 million hosts and more than 20 million users.[10]

The exponential growth of the Internet and our growing dependency on its use provides potential adversaries with an attractive medium to inflict IW attacks. In the Fall 1996 edition of *Soldier-Scholar*, Patrick Joula and Jonathan Reid notes the following:

> Most systems on the Internet are freely connected and can communicate with any other computer in the country—or the world. The vast majority of this information is sent in the clear, so that not only the designated recipient, but also any other machine or person who can obtain the text can read it. Recent incidents such as the Morris worm or the explosion of computer viruses have shown that the basic structure of the Internet is vulnerable to a skilled attack.[11]

Due to the amount of damage created by the Morris worm virus, specific details of the case are identified below:

> In 1988, Robert Morris, the son of the chief computer scientist at the National Security Agency created a software worm (a close cousin to a virus) and injected it into the Internet. This network-equipment virus attacked the UNIX operating system controlling the victimized Internet node, which spread the worm to its attached neighbors. The worm had a time-delayed reproduction so that it was hard to track. Eventually it cloned itself in computer centers all over the nation, causing an estimated $90 million in damage."[12]

Another example of our vulnerability is described in the Kevin Mitnik story. He is probably the most famous person in computer hacker history. According to Garry S. Howard, author of *Introduction to Internet Security: From Basics to Beyond*, he described Mitnik as follows:

> Mitnik started as a prankster, and then moved on to become a thief. His personal transformation almost coincides with the new trend leading from pranksters to malicious and vindictive destroyers of people and businesses. He made the transformation from dialing into computer installations to using the Internet to steal, abuse, and transport his electronic booty.
>
> Mitnik gained national attention when he broke into the Defense Department's computers, but his behavior degenerated, and he began altering credit reports of people who had offended him. He stole thousands of credit card numbers, ripped off critical information, stored it on stolen disk drive space, and tried to sell it to the highest bidders. With plenty of

> cash, he led the federal government on a long cyber-dragnet, which eventually failed. The federal agents employed a supercomputer programmer, a counter-hacker if you will, who helped to devise a strategy to eventually lure and capture Mitnik.[13]

The above examples represents activities conducted by U.S. citizens. Just imagine if our adversaries were able to duplicate this type of damage with intent on destroying our economic infrastructure. Wall Street would experience another "Black Monday." To proceed further, suppose our adversary was to infiltrate our air traffic control information systems or our major power grid sources, thus creating havoc in our airways and our cities. The possibility of these scenarios occurring is not unlikely. Consequently, our nation must be poised to identify and defeat this threat into the 21st century.

Summary

From the information presented in this chapter, undoubtedly the IW threat is a potential war-fighting strategy for the 21st century. This chapter focused specifically on the reality of the IW threat to our Armed Forces. The examples were used to highlight the nation's many vulnerabilities due to our growing dependency on information and information-based technologies. In a speech to the Armed Forces Communications and Electronics Association (AFCEA) in April 1995, General Ronald Fogleman, USAF chief of staff stated "...dominating the information spectrum is going to be critical to military success in the future."[14] Additionally, Joint Vision 2010 declares that in order to preserve our national interests, "we must have information superiority."[15] The reality of the IW threat requires that the DOD, the Joint Staff, and the Services create organizations capable of combating this threat. The next chapter will examine the activities of these specific organizations as they relate to IW.

Notes

[1]Joint Vision 2010, 11.

[2]Hans Binnendijk, "A Strategic Assessment for the 21st Century," in Joint Force Quarterly (Washington, DC, 1996) 68.

[3]JCS Publication, *Information Warfare: Legal, Regulatory, Policy and Organization Considerations for Assurance*; research report by SAIC for J6K, 4 July 96, A-176.

[4]Mr Emmett Paige, Jr., ASD/C4I, *Electronic Warfare and Information Warfare for Modern Military Applications*, Speech to 33rd Annual Association of Old Crows, International EW Technical Symposium and Convention, Washington Hilton and Towers, Washington DC, 1 Oct 96, internet.

[5]JCS Publication, *Information Warfare: A Strategy for Peace...The Decisive Edge in War* (JCS Publication, 1997) 9.

[6]Martin van Creveld, *The Transformation of War* (The Free Press, 1991) 196.

[7]SIGNAL Magazine, *Defense Organization Safeguards War Fighter's Information Flow*, October 1995, 16.

[8]Ibid., 16.

[9]Ibid., 15.

[10]Ibid., 18.

[11]Quoted in Soldier-Scholar: A Journal of Contemporary Military Thought, Patrick Joula and Jonathan Reid, *Civilian Cryptography and the Promise of Decentralization* (34th Education Squadron, USAF Academy, 1996) 45.

[12]Quoted in *Introduction to Internet Security: From Basics to Beyond by Garry S. Howard* (Prima Publishing, 1995) 21.

[13]Ibid, 20-21.

[14]Speech, AFCEA, Gen Ronald Fogleman, (*The Fifth Dimension of Warfare*, Washington, DC, April 1995)

[15]Joint Vision 2010, 16.

Chapter 4

Combating the Threat

Just as we prepare for a conventional weapons attack, we must be ready for attacks on our computer networks.

—Retired Senator Sam Nunn

The preceding chapters discussed the reality of the Information Warfare (IW) threat and how the threat will influence future war-making strategies. Thus, considerable efforts on the part of the Department of Defense (DOD), the Joint Staff, and the Services are taking place to combat the IW threat in the 21st century. Since DOD first published the official definition of IW, these organizations have established offices of primary responsibility for IW. This chapter will discuss those organizations and the progress made to date.

Department of Defense

Information Warfare Executive Board

Mr. John White, Deputy Secretary of Defense chairs an Information Warfare Executive Board (IWEB). "The purpose of the board is to provide a forum for the discussion and advancement of IW strategies, operations, and programs involving DOD."[1] Some of the board's responsibilities are shown below:

- Provide advice and recommendations to the DEPSECDEF and to the ASD (C3I) in his capacity as the DOD Information Warfare Manager.
- Provide for integrated development and considerations of IW policy, strategy, vulnerabilities and capabilities in all DOD activities.
- Eliminate gaps, identify overlaps, and ensure reciprocity in IW programs and operations.
- Serve as the forum for establishing coordinated DOD positions and recommendations on IW programs and operations, including interagency policy and strategy.
- Serve as the focal point for discussion of DOD IW policy, capabilities, and equities with national agencies, including recommending IW issues for consideration in the National Security Strategy.
- Focus Department and national level IW strategy, capitalizing on information technology to accomplish national security goals and objectives.[2]

The board's membership is shown in figure 4.

•Deputy Secretary of Defense (Chairman)	•Under Secretary of Defense (Acquisition)
•Under Secretary of Defense (Policy)	•Under Secretary of Defense (Comptroller)
•Under Secretary of Defense (Personnel & Readiness)	•Assistant Secretary of Defense for C3I
•Vice Chairman, Joint Chiefs of Staff	•General Counsel of the Dept. of Defense
•Vice Chiefs of the Military Services	•Director, Defense Info Sys Agency
•Director, National Security Agency	•Director, Defense Intelligence Agency
•Director, Program Analysis & Evaluation	•Deputy Director, CIA
•Executive Director, CIA	•National Security Council Executive

Source: *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, 2nd Edition, 4 July 1996, A-16.

Figure 4: IWEB Membership

Assistant Secretary of Defense for C3I

The Assistant Secretary of Defense for Command, Control, Communications and Intelligence ASD(C3I) serves as the principal IW advisor to the Secretary of Defense. This office was responsible for publishing the first official IW definition. The ASD(C3I) has established a Directorate for IW whose function is to conduct coordination, centralized planning, and oversight for IW.

Lieutenant General (ret) Emmett Paige, Jr., the current ASD(C3I) is a strong advocate of defensive IW policy and is presently coordinating a formal defensive IW strategy. He also supports a single agency manager for all telecommunications and information networks. Additionally, the ASD(C3I) is supporting an active Red Team effort. "The Red Team program is designed to increase awareness throughout DOD of the vulnerabilities of automated systems and improve the overall security posture."[3] The Joint Command and Control Warfare Center (JC2WC) at San Antonio, Texas is the executive agent for the DOD IW Red Team effort.

Joint Staff

The Joint Staff is the lead agency for developing IW joint doctrine. This doctrine includes both offensive and defensive measures. *Information Warfare: A Strategy for Peace...Decisive Edge in War* is the most recent joint IW publication highlighting the Joint Staff's IW vision.

The Directorate for Operations (J3), and the Directorate for Command, Control, Communications and Computer Systems (J6), share joint responsibility for IW. Responsibility for offensive IW lies with the J3 Information Warfare Special Technical Operations Division (IW/STOD), while J6 is responsible for all national information assurance and defensive information warfare programs and activities coordinated by the Joint Staff.[4] Currently, the J6 is leading an effort to develop rigorous modeling and simulation capabilities that would support commanders' requirements for awareness of vulnerabilities of supporting infrastructures. At the time of this writing, a Mission Needs Statement (MNS) for this capability was in final coordination.[5]

The Services

Army

Information Operations is the term the Army uses to describe its vision for Information Warfare policy and doctrine. The Army defines Information Operations as:

> Continuous military operations within the military information environment that enable, enhance, and protect the commander's decision cycle and mission execution to achieve an information advantage across the full range of military operations.[6]

According to the Air Land Sea Application Center's Information Warfare/Information Operations Study, the Army selected Information Operations rather than Information Warfare/Command and Control Warfare (C2W) for two reasons:

> First, the Army is firmly engaged in planning for the future. The digitized battlefield is the linchpin of the Army's Force XXI vision, allowing seamless C2 from the Corps commander to the soldier in the foxhole. Inherent in this vision is the need to gain and maintain information dominance, which gives Army commanders the ability to access the information required to synchronize battlefield actions.
>
> Secondly, the Army feels that the term Information Warfare is too restrictive. Using the term warfare implies that Information Warfare is restricted to combat operations. The Army developed the Information Operations concept to recognize the fact that information permeates the full range of military operations, beyond just the traditional context of warfare, from peace through global warfare. In the Army's view, the need to affect the flow of information extends beyond the traditional battlefield, and involves more than targeting the adversary's information systems while protecting our own. It also requires awareness and sensitivity to non-military information sources that can ultimately impact the overall campaign. Therefore, Information Operations expands the commander's battlespace, and includes worldwide interaction with the media, industry, joint forces, multinational forces, and computer networks.[7]

The Army's key response activity for Information Operations is the Land Information Warfare Activity (LIWA) established in March 1995 at Fort Belvoir, Virginia. Some of LIWA functions involve: providing support teams to facilitate operational planning and

conducting Army vulnerability assessments; and providing computer emergency response teams and Red Teaming.[8]

Through planned tests, exercises and demonstrations, the Army is conducting Red Team attacks on its own C3 and tactical information systems. "Using offensive IW technology that potential adversaries are believed to possess, the Army will seek to determine realistic vulnerabilities of its systems to attacks."[9]

Navy

According to Dr. Marvin Langston, deputy assistant secretary of the Navy for C3I, "information warfare has a growing emphasis within the Navy."[10] The Navy is currently incorporating IW into its doctrine of *"Forward...From the Sea."* The Navy defines IW as:

> The actions taken in support of national security strategy to seize and maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems.[11]

The Deputy Chief of Naval Operations for Plans, Policy and Operations (N3/N5) is responsible for developing Navy IW/C2W policy, strategy and operational concepts including operations security (OPSEC).

The Navy's principal agency for development of IW/C2W tactics, procedures, and training is the Fleet Information Warfare Center (FIWC). The FIWC was established on 1 Oct 1995 at Little Creek Amphibious Base, VA with a separate FIWC detachment in San Diego, CA. The purpose of FIWC is described below:

> FIWC deploys personnel trained in IW protect disciplines and equipped with appropriate hardware, including C2 protect hardware and software systems, to support battle group and joint task force operations. Additionally, FIWC provides Navy Computer Incident Response Teams

(NAVCIRT), and acts as the Navy's single point of contact for information systems monitoring.[12]

Another key Naval IW organization is the Navy's Information Warfare Activity (NIWA) located at Fort Meade, Maryland. The NIWA has two subordinate organizations: the Naval Research Laboratory in Washington, D.C., and the National Maritime Intelligence Center in Suitland, Maryland. The NIWA serves as the Navy's technical agent for the pursuit of IW related technologies. More specifically, NIWA conducts research and development into techniques that can be used to support IW.[13]

Marine Corps

In a SIGNAL magazine article in July 1996, Major Robert Wiedower, United States Marine Corps said "The Marine Corps is in the final stages of developing an IW policy and is instituting training and education throughout its service schools."[14] Headquarters, US Marine Corps (HQMC), Plans, Policy, and Operations is directly responsible for providing IW policy and guidance. The HQMC Command, Control, Communications, Computers, and Intelligence (C4I) Directorate is charged with developing information security and computer security policy.

The Marine Corps approach to IW/C2W is explained below:

> The Marine Corps approach to IW/C2W is based on two major service philosophies, operational focus and naval character. First, the Marine Corps is an operational force. Tactics, doctrine, and procedures are designed to allow them to win quickly and decisively on the operational and tactical battlefield. The Marine Corps views C2W as those actions taken by military commanders to realize the practical effects of IW on the battlefield. This view is particularly well suited to complement other Marine Corps concepts of maneuver warfare and "*Forward...From the Sea.*" Therefore, the Marine Corps has focused its efforts on C2W, and on integrating C2W into all operational plans.[15]

Air Force

In 1995, the Air Force published *Cornerstones of Information Warfare* which documents its initial philosophy on IW. There are several directorates at the Air Staff level working various aspects of IW; however, the Deputy Chief of Staff for Operations (XO) has the lead for coordinating IW doctrine in the Air Force.

In October 1993, the Air Force established the Air Force Information Warfare Center (AFIWC) at Kelly AFB in San Antonio, Texas. AFIWC's mission is described below:

> AFIWC's mission is to develop, maintain, and deploy IW/C2W capabilities in support of operations, campaign planning, acquisition, and testing. The Center acts as the time-sensitive, single focal point for intelligence data and C2W services. It provides technical expertise for computer and communications security and is the Air Force's focal point for tactical deception and operations security training.[16]

AFIWC created the Air Force Computer Emergency Response Team (AFCERT) to serve as the single point of contact in the Air Force for reporting and handling computer security incidents. The mission of the AFCERT is detailed below:

> The AFCERT deploys incident response teams to recover networked computer systems under attack from unauthorized sources. AFCERT Advisories are furnished to all users providing the latest information on system vulnerabilities and applicable countermeasures. The AFCERT coordinates computer security-related activities with all outside agencies and provides technical support to the Air Force Office of Special Investigations (AFOSI) during criminal and counter-intelligence investigations.[17]

In October 1995, the Air Force established its first IW squadron at Shaw Air Force Base, South Carolina. The squadron's mission involves conducting both offensive and defensive IW measures in support of the Air Operations Center. The squadron is a first step in establishing unit level support activities. The Air Force is envisioning creating more IW squadrons in the future.

Summary

This chapter focused primarily on IW organizations established by the DOD, the Joint Staff and the Services in response to potential IW threats. Despite budget constraints and manpower reductions, the organizations addressed in this chapter are very proactive in combating the threat. From newly formed IW offices to 24-hour computer response teams, these organizations are posturing themselves to win the battle against IW into the 21st century.

It must be pointed out, however that combating the IW threat will require a joint effort on the part of all the organizations. From this chapter, we saw how several of the Services used different terminology and expressed different strategic views on IW. Never-the-less, the Services are exchanging information on how to best train and educate their member forces. According to the Joint Staff, "efforts are under way to integrate IW into all aspects of joint warfare with education, training, and IW exercises receiving primary focus."[18]

The final chapters will present a few recommendations as to how we can improve our ability to win the IW war, and provide a summary of the findings discussed throughout the paper respectively.

Notes

[1]*Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance,* 2nd Edition, 4 July 1996, A-15.

[2]Ibid., A-15 - A-16.

[3]Col Brian Fredericks, *Information Warfare: The Organizational Dimension* (U.S. Army War College, Carlisle Barracks, Pennsylvania, 7 Feb 96) 5.

[4]Ibid, 6.

[5]*Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance,* 2nd Edition, 4 July 1996, A-23.

Notes

[6]*The Army Enterprise Implementation Plan*, Department of the Army Publication, 8 Aug 94, 2-14.

[7]Air Land Sea Application Center, *Information Warfare/Information Operations Study*, 15 December 1995, 8-10.

[8]SIGNAL Magazine, *Rapid Technology Growth Spawns Land Information Warfare Activity*, July 1996, 51.

[9]SIGNAL Magazine, *Army Information Operations: Protect Command and Control,* July 1996, 47.

[10]SIGNAL Magazine, *Navy Doctrine: Systems Face Information Warfare Makeover,* July 1996, 57.

[11]*Information Warfare/Information Operations Study* (Air Land Sea Applications Center) 17.

[12]Ibid., A-38.

[13]SIGNAL Magazine, *Navy Doctrine: Systems Face Information Warfare Makeover,* July 1996, 57.

[14]*Marine Corps Information Warfare Combines Services' Needs, Defines Their Differences* (SIGNAL Magazine, July 1996) 61.

[15]Information Warfare/Information Operations Study (Air Land Sea Applications Center, 15 Dec 95) 20.

[16]*Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance* (SAIC research product for J6K, Jul 96) A-57.

[17]Ibid., A-57.

[18]*Information Warfare: A Strategy for Peace...The Decisive Edge in War* (JCS Document, 1997) 15.

Chapter 5

Recommendations

> *There will continue to be states or groups that oppose or threaten American interests and values or those of our friends and allies. Our recognition of these threats and challenges will continue to drive our national security efforts.*
>
> —Joint Vision 2010

Survival in the 21st century will require additional efforts on the part of government and non-government agencies to combat the IW threat. Our nation's growing dependency on information and information-based technologies has made IW a legitimate weapon for potential adversaries. The "information" and its support infrastructures are becoming extremely vulnerable to hostile attacks. Adversarial forces can now wage information-based warfare from anywhere in the world, and literally remain anonymous. Thus, our ability to recognize and defend against this new form of warfare is paramount to the survival of our national security infrastructure. Thus, this chapter will address some of the recommendations that will aid in the fight against this new threat.

First, there must be a more concentrated effort on the part of DOD to integrate all IW activities. The Services are presently pursuing their own individual agendas to combat the IW threat; however, there needs to be a conduit that brings all of these individual efforts together to produce a overall joint synergistic IW strategy. Budget constraints will not allow the Services to continue down separate paths.

Secondly, education of our Armed Forces to the vulnerabilities inherent in the conduct of information transmission and reception remains a number one priority. Numerous computer intrusion incident reports reflect an alarming neglect for computer security and information security. Educating the populace on computer hacking techniques will aid in combating the IW threat in the 21st Century. Appendix A contains some of the most common techniques used by hackers to infiltrate computer systems.

Thirdly, combatant commanders must incorporate IW into their major exercise schedule. IW tasks should be incorporated into the Universal Joint Task Lists (UJTL). Additionally, combatant commanders must make IW tasks a part of their Joint Mission Essential Task Lists (JMETL). IW must remain at the forefront of the commander's tasking matrix. Commander's must practice offensive and defensive IW measures in their exercises. Transition to war should be transparent to how a command conducts its exercises. Implementing IW tactics into a major exercise should add realism into the training. USACOM has taken the first step in making IW a part of its exercise scenarios.

Fourth, implementing simple protective countermeasures such as automated intrusion detection capabilities, hacker warning alarms, double-password protection, software firewalls, virus scan software, etc., would eliminate many of the simple invasions that have occurred. Several of the units responsible for conducting computer intrusion exercises state that many of the systems (that are attacked) fail to employ the simplest of protection techniques.

Fifth, IW must not be dismissed as merely a passing fade, nor should it conjure up such a fear that commanders' expend mega bucks to combat it. There must be a balance in developing one's IW strategy. Implementing IW protect measures is expensive.

Therefore, risk assessments must be made to determine what information requires protecting. For example, several years ago, several governmental offices disseminated classification surveys to determine the amount of classified being contained in each department. Once the survey was completed, it was discovered that much of the information labeled as classified had been declassified years prior.

Finally, from a national perspective, there must be more done to resolve the legal dilemmas involving the prosecution of IW criminals. Jurisdiction in computer crimes may transcend both state and national boundaries. "The law, particularly international law, is currently ambiguous regarding criminality in and acts of war on information infrastructures."[1] Douglas Waller, author of *Onward Cyber Soldiers* wrote:

> More perilous are the security concerns for the United States where a tyrant with inexpensive technology could unplug NASDAQ or terrorist hackers could disrupt an airport tower. Frivolous excitement over infowar may be shaken by an electronic Pearl Harbor. Last year the government's Joint Security Commission called United States vulnerability to infowar "the major security challenge of this decade and possibly the next century."[2]

Currently, there are no international treaties in place to govern either offensive or defensive IW measures. Thus, our policy makers must continue to work to resolve this issue.

Notes

[1]*Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance* (2nd Edition, 4 Jul 96) 1-5.

[2]Quoted in World Politics 96/97, Douglas Waller, *Onward Cyber Soldiers*, 26.

Chapter 6

Conclusions

Know your enemy and know yourself; therefore in a hundred battles you will never be in peril.

—Sun Tzu

Although Sun Tzu wrote the above principle of war in the third century B.C., military strategists worldwide continue to benefit from its eternal truth. The allies' victory in the Gulf War is a direct result of their ability to obtain and exploit critical information about their adversary. Thus, Operation DESERT STORM legitimized IW as a warfighting strategy. This chapter will now address some of the findings discovered throughout the course of this research.

As suggested by Alvin and Heidi Toffler, the information age is here. Information has fast become a strategic resource that will permeate every facet of warfighting into the 21st century. Old paradigms regarding conventional warfare will be challenged by IW enthusiasts. As implied in paragraph one, we learned valuable lessons from the Gulf War. Unfortunately, so did our potential adversaries. The very strategies that we exercised against the Iraqi Armed Forces could easily be targeted toward our Armed Forces. To once again quote the famous war strategist Sun Tzu, "Information gathering is of the essence in warfare—it is what the armies depend upon for their every move."[1] Thus, a

war-fighting strategy that focuses on protecting our information while denying our adversary access to his will be paramount to the success of our national security strategy.

Although there is much debate on the reality of the IW threat, the growing number of computer intrusions on government and non-government systems substantiate the fact that the threat is very real. Our nation's growing dependency on information and information-based technologies have made us very vulnerable to hostile attacks. Additionally, IW provides potential attackers with a "wall of anonymity." Attacks can be launched from sites worldwide, thus contributing to our difficulty in combating this threat.

However, as postulated in the paper, the DOD, the Joint Staff and the Services are actively engaged in committing resources to combat the IW threat. Despite budget constraints and manpower reductions, the organizations are very proactive in combating the threat. From newly formed IW offices to 24-hour computer response teams, these organizations are posturing themselves to win the battle against IW into the 21st century.

It must be pointed out, however that combating the IW threat will require a joint effort on the part of all the organizations. From this paper, we saw how several of the Services used different terminology and expressed different strategic views on IW. Never-the-less, the Services are exchanging information on how to best train and educate their member forces.

While this paper focused primarily on DOD, the Joint Staff and the Services' involvement in IW, it clearly recognizes the importance of non-government and the commercial sector's role in combating this threat. No element of society is immune from potential IW attacks. From the bombing of the World Trade Center in New York to the explosion in the Kobar Towers in Saudi Arabia, terrorists continues to wage war against

American interests. Unfortunately, IW has now given them another tool to exploit. As a nation destined to remain the only super power in the 21st century, we cannot afford to dismiss the reality of this new wave of warfare - to do so would be to our own peril.

Notes

[1]Sun Tzu, *The Art of War*, 17.

Appendix A

Computer Hacking Techniques

Computer hackers use various techniques to infiltrate your computer. In his book, Introduction to Internet Security: From Basics to Beyond, Garry S. Howard describes some of the techniques.[1]

Name of Technique	Description of Technique
•Scavenging	•The simple act of looking for valuable data, whether the information is on-line, stored in tapes or disks off-line, or on printouts in the dumpster.
•Impersonators/Piggybackers	•Individuals "slip" through security doors by pretending to have their hands full, or they introduce themselves as "reporters" to get full tours of computer facilities. Or an impersonator can use an phony terminal, wait for the real user to sign off, and then use the unattended terminal to gain access.
•Wiretapping	•This involves tapping of telephone lines, computer parts, modem ports, or other hardware, but it's also possible to "eavesdrop" or "tap" someone's communication input/output buffers or memory areas so that whatever is being sent or received can also be recorded by unknown parties.
•Data Diddling	•This technique uses the complex codes in the computer to direct funds or other valuable resources to an unauthorized account. The numeric codes often conceal where the funds are taken from, so "diddling" is often hard to find if applications don't permit easy auditing of funds distribution.
•Salami Slicing	•This technique is used to "skim" funds secretly form one account to another, so that one person or organization receives the funds in their account. The salami-thief may be able to make repeated small electronic transfers of small change from thousands of accounts.
•Superzaps	•When a systems programmer loads a special operating system and then uses expanded system privileges to access privileged files and transfer money from one account to another, it is called a "superzap."
•Asynch Attacks	•When programs pause in main memory, hackers can sometimes access their data and use them to penetrate the system.

—Continued

Name of Technique	Description of Technique
•Simulation and Modeling	•Some hackers actually use a company's own computer to model or simulate the necessary adjustments necessary to hide their theft.
•Trojan Horses	•Trojan horses are viruses hidden inside of software. They may damage or erase data files and programs, but they may also display messages or images and steal money from computer accounts and anonymously send email to the hacker who introduced the virus. "Worms" are similar but designed to spread through a network, consuming memory or disk space in a node until it fails. A new virus type, called a cruise virus, attacks a specific target on a network or computer.
•Back Doors	•Systems programmers of network and computer systems often have secret passwords to gain operational control of a computer or piece of network equipment. These passwords are normally easy to break, allowing hackers to do incredible damage and theft.
•Trap Doors	•Often, programmers will build "hacker routines" into their programs, taking advantage of the program's access to critical areas of memory, CPU registers, and disk space to perform functions not available to interactive users.
•Logic Bombs	•At a system time or date, or after a certain event on the system (i.e. execution of a certain program, particular user logs on, after disk space consumption reaches a specific level, or after any other event trackable through the system) a destructive act is done. It could be erasure of disks, system shutdown, or viral incubation and proliferation.
•Password Busting	•This is a technique to find secret passwords. Some hackers use random number generators, special password analysis software, or other techniques, combined with repeated calling of the same dial-up computer to gain unauthorized access to a host.

Notes

[1]Garry S. Howard, *Introduction to Internet Security: From Basics to Beyond*, (Prima Publishing, 1995) 104.

Glossary

Assurance. A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. If the security features of an AIS are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during AIS operation. [DODD 5200.28, 1988]

Attack Assessment. An evaluation of information to determine the potential or actual nature and objectives of an attack for the purpose of providing information for timely decisions. [CJCS Joint Pub 1-02, March 1994]

Classified National Security Information. Information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. [Executive Order 12958, April 1995]

Command and Control Warfare (C2W). The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions. Command and Control Warfare applies across the operational continuum and all levels of conflict. Also called C2W. C2W is both offensive and defensive. [CJCS MOP 30, 1993]

Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, and physical security of COMSEC material. [NSTISSI 4009, 1992]

Critical Infrastructures. Infrastructures that are deemed to be so vital that their incapacity or destruction would have a debilitating regional or national impact. They include at least seven categories: telecommunications; electrical power systems; gas and oil; banking and finance; transportation; water supply systems; continuity of government and government operations. Emergency services (including medical, police, and rescue services) might also be considered critical infrastructures. [Information Warfare: Legal, Regulatory, Policy and Organization Considerations for Assurance, July 1996]

Damage to the National Security. Harm to be national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information. [Executive Order 12958, April 1995]

Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communications, interpretation, or processing by humans by automatic means. Any representations such as characters or analog quantities to which meaning is, or might be, assigned. [Information Warfare: Legal, Regulatory, Policy and Organization Considerations for Assurance, July 1996]

Defense Information Infrastructure (DII). The DII encompasses information transfer and processing resources, including information and data storage, manipulation, retrieval, an display. More specifically, the DII is the shared or interconnected system of computers, communications, data applications, security, people, training, an other support structure, serving the DOD's local and worldwide information needs. [ASD(C3I) Memo, 1994]

Defense Information Systems Network (DISN). The DISN is the DOD's consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner. [ASD(C3I) Memo, 1994]

Defensive Counterinformation. Actions protecting our military information functions from the adversary. [Air Force Cornerstones of Information Warfare, Aug 95]

Defensive Information Warfare (IW-D). Process that integrates and coordinates policies and procedures, operations, intelligence, law, and technology to protect information and defend information systems. [CJCSI 6510.01A, 1996]

Denial of Service. Action or actions that result in the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of operational capability. [DODD 5200.28, 1988]

Electronic Warfare (EW). Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. [Joint Pub 1-02, 1994]

Global Information Infrastructure (GII). Includes the information systems of all countries, international and multinational organizations and multi-international commercial communications services. [Information Warfare: Legal, Regulatory, Policy and Organization Considerations for Assurance, July 1996]

Hacker. Unauthorized user who attempts or gains access to an information. [NSTISSI No. 4009, January 1996]

Identification and Authentication. Verification of the originator of a transaction, similar to the signature on a check or a Personal Identification Number on a bank card. [CJCSI 6510.01A, 1996]

Information. Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium. [Information Warfare: Legal, Regulatory, Policy and Organization Considerations for Assurance, July 1996]

Information Assurance. The availability of services and information integrity. [Information Warfare: Legal, Regulatory, Policy and Organization Considerations for Assurance, July 1996]

Information Integrity. The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed. [Executive Order 12958, April 1995]

Information Security. The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. [FED-STD-1037B, 1991]

Information Superiority. That degree of dominance in the information domain which permits the conduct of operations without effective opposition. [DODD 3600.1, 1995]

Information System. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. [DODD 3600.1, 1995]

Information Systems Security. The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. [NSTISSI 4009, 1992]

Information Warfare (IW). Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. [CJCSI 3210.01, 1996]

Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, to the smooth functioning of governments at all levels, and to society as a whole. [Information Warfare: Legal, Regulatory, Policy and Organization Considerations for Assurance, July 1996]

Local Area Network (LAN). A data communications system allowing a number of independent devices to communicate directly with each other, within a limited sized geographic area over a physical communications channel. [IEEE]

National Communications System. The telecommunications system that results from the technical and operational integration of the separate telecommunications systems of the several executive branch departments and agencies having a significant telecommunications capability. [Joint Pub 1-02]

National Military Command System. The priority component of the Worldwide Military Command and Control System (replaced by the Global Command and Control System) designed to support the National Command Authorities and Joint Chiefs of Staff in the exercise of their responsibilities. [Joint Pub 1-02]

National Information Infrastructure (NII). It is a system of high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It also includes public and private networks. [NII Security: The Federal Role, 1995]

Bibliography

Ackerman, Robert K. "Businesses Face Threat of Information Warfare." *SIGNAL Magazine*, June 1996, 45-46.

Ackerman, Robert K. "Marine Corps Information Warfare Combines Services' Needs,Defines Their Differences." *SIGNAL Magazine,* July 1996, 61-62.

Ackerman, Robert K. "Navy Doctrine, Systems Face Information Warfare Makeover." *SIGNAL Magazine*, July 1996, 57-60.

Air Land Sea Applications Center. *Information Warfare/Information Operations Study.* Staff study, 15 December 1995.

Aldrich, Maj Richard W. "The International Legal Implications of Information Warfare." *Air Power Journal,* Fall 1996, 99-109.

Allard, Kenneth. *Command, Control, and the Common Defense.* Revised ed. Washington D.C.: National Defense University Press, 1996.

Baucom, Lt Col Donald R. "The Mechanization of Land Warfare: Ideas, Technology, and Weapons." *Air Command and Staff College Correspondence Book.* Vol. 3. Ver. 9. 1993, 10-77.

Binnendijk, Hans. "A Strategic Assessment for the 21st Century." *Joint Force Quarterly* (Autumn 96) 68.

Braunberg, Andrew C. "Air Force Pursues Two-Sided Information Warfare Strategy." *SIGNAL Magazine*, July 1996, 63-65.

Buchan, Glen. *"Information War and the Air Force: Wave of the Future? Current Fad?"* Issue Paper. RAND Corporation Publication, March 1996.

Campen, Alan D. *The First Information War.* Fairfax, VA.: AFCEA International Press, 1992.

Clancy, Tom. *Debt of Honor.* New York, N.Y.: G.P. Putnam's Sons Publishers, 1994.

Cornerstones of Information Warfare. Washington, D.C.: Government Printing Office, 1995.

Creveld, Martin van. *The Transformation of War.* New York, N.Y.: The Free Press, 1991.

Fadok, Maj David S. *John Boyd and John Warden, Air Power's Quest for Strategic Paralysis.* Montgomery AL.: Air University Press, 1995.

Fogleman, Gen Ronald R. chief of staff, US Air Force. *"The Fifth Dimension of Warfare."* Speech. Armed Forces Communications-Electronics Association (AFCEA), Washington, D.C., April 1995.

Fredericks, Col Brian. *Information Warfare: The Organizational Dimension.* Research Report no. 19960620-096. Carlisle Barracks, PA.: U.S. Army War College, 1996.

Gilder, George. *Microcosm: The Quantum Revolution in Economics and Technology.* New York, N.Y.: Simon and Schuster, 1989.

Greene, Brent. "President's Commission on Critical Infrastructure Protection. Trends Leading to New Vulnerabilities." Briefing. Air Command and Staff College, Maxwell AFB, AL, 18 Mar 97.

Grier, Peter. "At War With Sweepers, Sniffers, Trapdoors, and Worms." *Air Force Magazine*, March 1997, 20-24.

Horizon '95: C4I, A Vision for the Future. Washington, D.C.: Government Printing Office, 1995.

Howard, Garry S. *Introduction to Internet Security: From Basics to Beyond.* Rocklin, CA.: Prima Publishing, 1995.

Information Warfare. Washington, D.C.: Government Printing Office, 1996.

Jensen, Col Owen E. Information Warfare: Principles of Third Wave War. *Air Power Journal,* Fall 1994, 36.

Joula, Patrick and Jonathan Ried. "Civilian Cryptography and the Promise of Decentralization." *Soldier-Scholar: A Journal of Contemporary Military Thought,* Vol. 3, no. 1, Fall 1996, 43-47.

Libicki, Martin C. *Protecting the United States in Cyberspace.* Washington, D.C.: National Defense University Press, 1996.

Libicki, Martin C. *What is Information Warfare?* Washington, D.C.: National Defense University Press, 1995.

Maxwell, Arthur G. Jr. *Joint Training for Information Managers.* Washington, D.C.: National Defense University Press, 1996.

Office of the Joint Chiefs of Staff. *C4I: Global Command & Control System.* Washington, D.C.: Government Printing Office, 1994.

Office of the Joint Chiefs of Staff Joint Pub 6-0. *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations.* Washington, D.C.: Government Printing Office, 30 May 1995.

Office of the Joint Chiefs of Staff. *Information Warfare. Legal, Regulatory, Policy and Organizational Considerations for Assurance* 2nd ed. Washington, D.C.: Government Printing Office, 1996.

Office of the Joint Chiefs of Staff. *Information Warfare: A Strategy for Peace...The Decisive Edge in War.* Washington, D.C.: Government Printing Office, 1996.

Office of the Joint Chiefs of Staff. *Joint Vision 2010.* Washington, DC: Government Printing Office, 1996.

Paige, Emmett, Jr. "Electronic Warfare (EW) and Information Warfare (IW) for Modern Military Applications." Speech. Old Crows International EW Technical Symposium and Convention, Washington, D.C., 1 October 1996.

Robinson, Clarence A. Jr. "Activating Firewall Security." *SIGNAL Magazine.* October 1995, 32-34.

Robinson, Clarence A. Jr. "Army Information Operations: Protect, Command and Control." *SIGNAL Magazine*, July 1996, 47.

Robinson, Clarence A. Jr. "Defense Organization Safeguards War Fighters' Information Flow." *SIGNAL Magazine.* October 1995, 15-18.

Robinson, Clarence A. Jr. "Information Warfare Strings Trip Wire Warning Strategy." *SIGNAL Magazine*, May 1996, 29-33.

Robinson, Clarence A. Jr. "Rapid Technology Growth Spawns Land Information Warfare Activity." *SIGNAL Magazine*, July 1996, 51-54.

Robinson, Clarence A. Jr. "Smart Cards Execute Security, Arrest Intruders' Data Access." *SIGNAL Magazine*, October 1995, 37-39.

Robinson, Clarence A. Jr. "Trusted Data Base Management Executes Multilevel Protection." *SIGNAL Magazine*. October 1995, 25-27.

Schwartau, Winn. *Chaos on the Electronic Superhighway: Information Warfare*. New York, N.Y.: Thunder's Mouth Press, 1994.

Stein, George J. "Information Warfare." *Airpower and Campaign Planning*. Vol. 8. Maxwell AFB, AL.: Air University Press, March 1997.

The Army Enterprise Implementation Plan. Washington, D.C.: Government Printing Office, 1994.

The Vision 1996: Army Enterprise Strategy. Washington, D.C.: Government Printing Office, 1996.

Toffler, Alvin and Heidi. *War and Anti-War. Survival at the Dawn of the 21st Century*. Boston, MA.: Little, Brown, and Company, 1993.

Wallace, LTC John and Maj Jim Jones. "Information Warfare/Information Operations (IW/IO) Update. *The Air Land Sea Bulletin*, Issue no. 96-1 (April 1996) 15-16.

Waller, Douglas. "Onward Cyber Soldiers." *Annual Editions: World Politics 96/97*. Guilford, Conn.: Dushkin Publishing Group/Brown & Benchmark Publishers, 1996.

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air Command and Staff College
Maxwell AFB, Al 36112